CLAIMS

What is claimed is:

1. An information hiding method with reduced fuzziness, which comprises the steps of:

Sub A1

inputting the information to be embedded into a spin encoder and generating encoded information whose length is a multiple of the original information;

generating a random number sequence using cross encoding for permuting the encoded information, the seed of the random numbers being a first key;

selecting a pixel of a host image using a random number generator as an information embedding point of the encoded information, the seed of the random number generator being a second key, and

embedding the encoded information into the B channel of the pixel of the host image.

2. The method according to claim 1, wherein the spin encoding corrects transmission errors or human damages on the encoded information.

3. The method according to claim 1, wherein the random number sequence is generated by a linear feedback shift register.

4. The method according to claim 3, wherein the linear feedback shift register comprises a plurality of buffers.

5. The method according to claim 1 further comprising the following steps for extracting the embedded information:

using the second key to compute the embedding positions of the encoded

information;

using the first key to reconstruct the encoded information and to restore the order before cross encoding; and

decoding the encoded information using spin decoding.

6. The method according to claim 1, wherein the host image H is an image of m×n pixels and the electronic signature to be embedded is information W with a size L, both the host image H and the embedded information W being expressed as:

$$H = \{h_{ij} \mid 0 \le i < m, 0 \le j < n, h_{ij} \in [0,255]\}, \textit{and}$$

$$W = \{w_i \mid 0 \le i < L, w_i \in [0,1]\}; \quad \textit{and}$$

a set $ASET_{ij}=\{h_{i+1,j}, h_{i-1,j+1}, h_{i,j+1}, h_{i+1,j+1}\}$ being defined for four pixels surrounding and to the right of any pixel h_{ij} in the host image.

7. The method according to claim 6, wherein a temporary variable is defined to be $h'=(h_{i-1,j-1}+h_{i,j-1}+h_{i-1,j+1}+h_{i-1,j}+h_{i+1,j}+h_{i-,j+1}+h_{i,j+1}+h_{i+1,j+1})/8$.

8. The method according to claim 6 further comprising the step of adjusting the values of $h_{i,j}$ and $ASET_{i,j}$ according to:

while(((h'-h_{ij} ≦ t) and (w=0)) or ((h_{ij}-h' ≦ t) and (w=1))) do

begin

for each $h_{i'j'} \in ASET_{ij}$ *do*

$h_{i'j'}=h_{i'j'}-2w+1$;

$h_{i,j}= h_{i,j}+2w-1$;

$$h'=(h_{i-1,j-1}+h_{i,j-1}+h_{i-1,j+1}+h_{i-1,j}+h_{i+1,j}+h_{i-,j+1}+h_{i,j+1}+h_{i+1,j+1})/8;$$

end.

Sub A1

9. The method according to claim 5, wherein the hidden information is true if $h' \leqq h_{i,j}$ in the step of using the second key to compute the embedding positions of the encoded information.

10. The method according to claim 5, wherein the spin decoding adopts the Viterbi algorithm.